

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開平11-66008

(43) 公開日 平成11年(1999) 3月9日

(51) Int. Cl. ⁸	識別記号	F I
G 0 6 F 15/00	3 3 0	G 0 6 F 15/00 3 3 0 G
A 6 3 F 9/22		A 6 3 F 9/22 G
G 0 6 F 12/14	3 2 0	G 0 6 F 12/14 3 2 0 F
17/60		15/21 3 4 0 B
G 0 7 F 7/12		G 0 7 F 7/08 B

審査請求 未請求 請求項の数 9 OL (全 11 頁) 最終頁に続く

(21) 出願番号 特願平9-231107

(22) 出願日 平成9年(1997) 8月27日

(71) 出願人 000132471

株式会社セガ・エンタープライゼス
東京都大田区羽田1丁目2番12号

(72) 発明者 川堀 昌樹

東京都大田区羽田1丁目2番12号 株式会
社セガ・エンタープライゼス内

(74) 代理人 弁理士 土井 健二 (外1名)

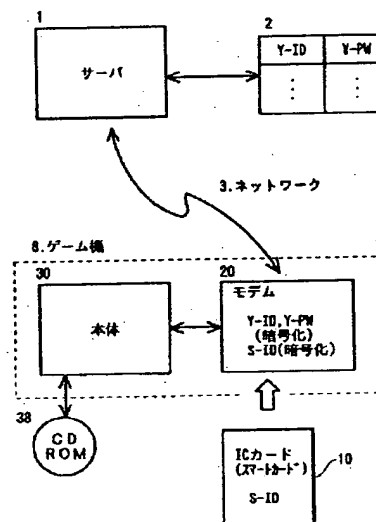
(54) 【発明の名称】 ICカードを利用したゲーム装置

(57) 【要約】

【課題】 認証情報である英数字をアクセスのたびに入力する煩雑さを解消する。

【解決手段】 本発明は、モデム装置が装着可能であって、モデム装置を装着してからサーバに通信回線を介して接続され、認証情報を送信してサーバで正規ユーザである認証を受けた時に、一定のサービスを受けることができるゲーム装置において、正規ユーザに与えられるICカードのカードIDと認証情報とが記録される記録媒体がモデム装置に設けられ、モデム装置に挿入されたICカードのカードIDが、記録媒体に記録されたカードIDと一致する時に、記録された前記認証情報が前記サーバに送信されることを特徴とする。ICカードのカードIDを鍵データにして、記録媒体への認証用情報の記録に鍵をかけることにより、不正使用に対する耐性を高くし、アクセスするたびに認証用の英数字を入力する煩雑さを解消することができる。

第一の実施の形態例の概略図



【特許請求の範囲】

【請求項1】サーバに通信回線を介して接続され、認証情報を送信してサーバで正規ユーザである認証を受けた時に、一定のサービスを受けることができる通信端末装置において、

前記正規ユーザに与えられるICカードのカードIDを鍵データにして、前記認証情報が記録される記録媒体を有し、

挿入されたICカードのカードIDを鍵データにして、前記記録媒体に記録された前記認証情報が前記サーバに送信されることを特徴とする通信端末装置。

【請求項2】サーバに通信回線を介して接続され、認証情報を送信してサーバで正規ユーザである認証を受けた時に、一定のサービスを受けることができる通信端末装置において、

前記正規ユーザに与えられるICカードのカードIDと前記認証情報とが記録される記録媒体を有し、

前記挿入されたICカードのカードIDが、前記記録媒体に記録されたカードIDと一致する時に、前記記録された前記認証情報が前記サーバに送信されることを特徴とする通信端末装置。

【請求項3】モデム装置が装着可能であって、該モデム装置を装着してからサーバに通信回線を介して接続され、認証情報を送信してサーバで正規ユーザである認証を受けた時に、一定のサービスを受けることができるゲーム装置において、

前記正規ユーザに与えられるICカードのカードIDと前記認証情報とが記録される記録媒体が前記モデム装置に設けられ、

前記モデム装置に挿入されたICカードのカードIDが、前記記録媒体に記録されたカードIDと一致する時に、前記記録された前記認証情報が前記サーバに送信されることを特徴とするゲーム装置。

【請求項4】請求項3において、前記記録媒体への認証情報の記録または消去が、前記ICカードが挿入されたことを条件に可能であることを特徴とするゲーム装置。

【請求項5】サーバに通信回線を介して接続され、使用許諾を要求するプログラムデータを送信し、前記サーバから使用許諾パスワードを受信し、所定のプログラムの使用を前記使用許諾パスワードによって使用可能にする通信端末装置において、

前記通信端末装置に挿入されたICカードのカードIDを前記サーバに送信可能であり、

前記サーバにて前記カードIDを鍵データにして暗号化された前記使用許諾パスワードが記録される記録媒体を有し、

挿入された前記ICカードのカードIDを鍵データにして前記記録媒体に記録された暗号化使用許諾パスワードが復号化されることを特徴とする通信端末装置。

【請求項6】請求項5において、

前記記録媒体は、前記カードIDも使用許諾パスワードと共に記録可能であり、前記挿入された前記ICカードのカードIDが前記記録されたカードIDと一致する時に、前記復号化が許可されることを特徴とする通信端末装置。

【請求項7】サーバと通信端末装置とが通信回線を介して接続可能に構成され、前記通信端末装置における所定のプログラムの使用を許可する使用許諾パスワードの管理方法において、

(a) 前記通信端末装置に挿入されたICカードのカードIDと共に前記プログラムのIDを、前記通信端末装置から前記サーバに送信する工程と、

(b) 前記サーバは、前記送信されたプログラムIDに対応する使用許諾パスワードを前記送信されたカードIDを鍵データとして暗号化し、該暗号化された使用許諾パスワードを前記通信端末装置に送信する工程と、

(c) 前記通信端末装置は、前記送信された暗号化された使用許諾パスワードを記録媒体に記録する工程と、

(d) 前記通信端末装置に挿入されたICカードに記録されたカードIDを鍵データにして、前記記録された暗号化使用許諾パスワードを復号化し、該復号化された使用許諾パスワードを使用して前記プログラムの使用をする工程とを有することを特徴とするプログラムの使用許諾パスワードの管理方法。

【請求項8】請求項7において、

更に、(e) 前記サーバは、前記カードIDと送信した使用許諾パスワードとの対応テーブルを記録する工程と、

(f) 前記通信端末装置から前記カードIDが送られた時、前記対応テーブルに記録された該カードIDに対応する使用許諾パスワードを前記カードIDにより暗号化して送信する工程とを有することを特徴とする使用許諾パスワードの管理方法。

【請求項9】請求項7において、

更に、(g) 前記サーバは、前記工程(b)において前記暗号化された使用許諾パスワードを前記通信端末装置に送信する時に、前記ICカードに記録されているクレジット度数を減少する工程と、

(h) 前記サーバは、前記カードIDに対応する最新のクレジット度数データを保管する工程と、

前記工程(a)において、前記通信端末装置は、挿入されたICカードのクレジット度数データも併せて前記サーバに送信し、

前記工程(b)において、前記サーバは、受信したクレジット度数データと前記保管された最新のクレジット度数データとを照合し、一致する場合に前記使用許諾パスワードを暗号化して送信することを特徴とする使用許諾パスワードの管理方法。

50 【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、ネットワークを介してセンタのサーバにアクセスする為のユーザのIDやパスワード等の個人認証のための情報を記録して、容易に送信可能にするとともに、その記録した個人認証の情報のセキュリティを高くすることができるゲーム装置または端末装置に関する。

【0002】

【従来の技術】送信機能を有するゲーム装置や端末装置をネットワークを介してセンタのサーバに正規ユーザであるか否かを認証する為の情報として、ユーザIDとそれに対するユーザパスワード等が送信される。そして、サーバ側では、予め登録されているユーザIDとユーザパスワードの照合を取り、正規ユーザか否かの認証を行う。

【0003】一般には、このユーザIDやユーザパスワードは、無意味な英数字の文字列であり、これらの文字列をネットワークのサーバに接続するたびにユーザがゲーム装置や端末装置から入力することは煩雑である。特に、ゲーム機の場合は、通常入力用のキーボードを有しておらず、接続したテレビ画面上に表示されたソフトウェアキーボードにより入力する必要がある、その場合は、英数字の入力は益々煩雑である。

【0004】また、ユーザの認証用の情報だけでなく、ゲームのプログラムを格納した記録媒体を流通させ、それぞれのゲームプログラムの各ステージ毎にパスワードを課金するたびにネットワークを通じてユーザに与えるゲームプログラムの超流通においても、ゲーム・パスワードを入力する必要がある。その場合も、そのゲーム・パスワードを毎回入力する作業はユーザにとって煩雑である。

【0005】

【発明が解決しようとする課題】上記のサーバに接続するたびに認証用の情報を入力したり、ゲームプログラムを実行するたびにゲーム・パスワードを入力する作業を省略する為に、それらの情報をゲーム機や端末装置内の不揮発性のメモリに記録する方法が考えられる。

【0006】しかしながら、単純にゲーム機や端末装置の不揮発性メモリに情報を記録すると、容易にコピーされ、それらの情報が正規ユーザからの情報であるか否かの個人認証のセキュリティが低くなることが問題となる。即ち、ゲーム機や端末装置の不揮発性メモリに情報を記録する方法では、ユーザがゲーム機や端末装置を所有していることを根拠にして認証を行うことになる。その為に、ゲーム機や端末装置の不正使用者に対して耐性の低いシステムとなる。また、多数のユーザがゲーム機や端末装置を共有するシステムにおいては、上記の方法では、ユーザの認証が適切に行われない。

【0007】そこで、本発明の目的は、通信機能を有するゲーム機や通信端末装置において、認証用の情報やパ

スワードをセキュリティが高く、不正使用に対して耐性が高く記録されるゲーム機または通信端末装置を提供することにある。

【0008】

【課題を解決するための手段】上記の目的を達成する為に、本発明は、サーバに通信回線を介して接続され、認証情報を送信してサーバで正規ユーザである認証を受けた時に、一定のサービスを受けることができる通信端末装置において、前記正規ユーザに与えられるICカードのカードIDを鍵データにして、前記認証情報が記録される記録媒体を有し、挿入されたICカードのカードIDを鍵データにして、前記記録媒体に記録された前記認証情報が前記サーバに送信されることを特徴とする。

【0009】ICカードのカードIDを鍵データにして、記録媒体への認証用情報の記録に鍵をかけることにより、不正使用に対する耐性を高くし、アクセスするたびに認証用の英数字を入力する煩雑さを解消することができる。

【0010】また、上記の目的を達成する為に、本発明は、サーバと通信端末装置とが通信回線を介して接続可能に構成され、前記通信端末装置における所定のプログラムの使用を許可する使用許諾パスワードの管理方法において、(a)前記通信端末装置に挿入されたICカードのカードIDと共に前記プログラムのIDを、前記通信端末装置から前記サーバに送信する工程と、(b)前記サーバは、前記送信されたプログラムIDに対応する使用許諾パスワードを前記送信されたカードIDを鍵データとして暗号化し、該暗号化された使用許諾パスワードを前記通信端末装置に送信する工程と、(c)前記通信端末装置は、前記送信された暗号化された使用許諾パスワードを記録媒体に記録する工程と、(d)前記通信端末装置に挿入されたICカードに記録されたカードIDを鍵データにして、前記記録された暗号化使用許諾パスワードを復号化し、該復号化された使用許諾パスワードを使用して前記プログラムの使用をする工程とを有することを特徴とする。

【0011】ICカードのカードIDを鍵データに利用してプログラムの使用許諾パスワードを暗号化して通信端末装置のメモリに記録するので、使用許諾パスワードそのものをユーザに開示することなく、そのサービスを提供することができる。また、記録しておくことで、プログラムを使用するたびに使用許諾パスワードを入力する煩雑さは解消される。しかも、ICカードと通信端末装置の記録媒体とを物理的に分離することで、不正使用に対する耐性を高くすることができる。

【0012】

【発明の実施の形態】以下、本発明の実施の形態について図面に従って説明する。しかしながら、本発明の技術的範囲がその実施の形態に限定されるものではない。

【0013】【第一の実施の形態例】個人認証の情

報) 図1は、第一の実施の形態例の全体構成を示す図である。第一の実施の形態例では、個人認証用の情報をゲーム機や通信端末装置の不揮発性メモリに記録し、且つ、一般に複製が困難なICカード(別名スマートカード)に記録されているICカードに固有の情報を鍵データにして、その記録に電子的な鍵をかける。

【0014】図1に示される通り、サーバ1に電話回線等のネットワーク3を介してゲーム機6が接続される。本発明はゲーム機だけでなく通信端末装置から認証情報を送信する場合にも適用できるが、ここではゲーム機を例にして説明する。図1の例では、ゲーム機6の本体30には通信機能がないので、それに接続されるモデム20を介してサーバ1と接続される。但し、モデム20が本体30と一体化されてゲーム機6が構成されても良い。そして、ゲーム機6内のモデム20内の不揮発性メモリ内に、認証用の情報であるユーザIDとそれに対するユーザパスワードとが記録される。このモデム20内の不揮発性メモリ内の情報は、一般に読み出しが困難な状態にある。

【0015】更に、重要なことは、正規ユーザのみが所有するICカード10のユニークなID(スマートカードのIDとして以下S-ID)を鍵にして、モデム20内の不揮発性メモリ内に記録された認証情報の記録に電子的な鍵がかけられる点にある。即ち、モデム20内の不揮発性メモリ内に、ユーザID:Y-ID、ユーザパスワードY-PWに加えて、ICカードのIDとしてS-IDを記録する。そして、ゲーム機6に正規ユーザが所有するICカードが装着されて、そのカードのIDであるS-IDとモデム20内の不揮発性メモリに記録されているカードID:S-IDとが一致する場合のみ、個人認証用のユーザID:Y-IDとユーザ・パスワードY-PWとがネットワークを通じてサーバ1に送信される様にする。

【0016】ここで、ICカード10は、例えばネットワークを介してゲーム機6をサーバ1に接続し、ゲームプログラムの使用のサービスを受けたり、別途流通させたゲームプログラムを格納した記録媒体38の使用許諾パスワードを受信するサービスを受ける時の、課金に利用される。即ち、予めサービスを利用する為の料金の支払いを条件にICカードがプリペイドカードとして正規のユーザに譲渡される。従って、本実施の形態例ではその正規ユーザが所有するICカード内のユニークな情報であるカードID:S-IDを、電子的な鍵データとして利用する。

【0017】この方式によれば、ICカードを所有する正規ユーザが、同様に正規ユーザが所有するゲーム機6を使用する場合のみ、不揮発性メモリ内に記録された認証用の情報であるユーザID:Y-IDとユーザパスワードY-PWとがサーバ1に送信されるので、非常にセキュリティが高く、不正使用者に対する耐性が高いシス

テムとなる。認証用情報とICカードID:S-IDとは、モデム20内の不揮発性メモリでなく、ゲーム機の本体30内のメモリに記録される場合でも良いが、それらの情報の複製を困難にするためには、モデム20内の不揮発性メモリに記録するのが適切である。

【0018】更に、この方式によれば、正規ユーザが第三者にICカードとゲーム機6またはモデム20を貸与することにより、第三者に認証用の情報を開示することなく、ネットワークを通じての所定のサービスを第三者に受けることを許可することができる。従って、店頭などで不特定多数のユーザに対して、ネットワークを介してサーバ1に接続したデモを提供することが可能になる。

【0019】また、モデム20内の不揮発性メモリに認証用情報やICカードIDを記録する場合、ゲームプログラムが格納された記録媒体38内に格納されているゲームプログラムに共通する鍵データを利用して、認証用情報Y-ID、Y-PWやICカードID:S-IDを暗号化して記録することもできる。

【0020】尚、サーバ1側では、ユーザID:Y-IDとユーザ・パスワードY-PWとの照合を行う為のテーブルがファイル装置2に記録される。サーバ1では、送信されるユーザID:Y-IDとユーザ・パスワードY-PWとの照合を上記ファイル装置2内のテーブルを参照することで行い、正規ユーザか否かの認証を行う。

【0021】図2は、ゲーム機とIDカードの詳細構成を示す図である。この例では、テレビ等のモニタ画面40に接続されるゲーム本体30に、通信機能を付加する為のモデム装置20がモデムスロット31に挿入可能になっている。更に、そのモデム装置20にプリペイドカードなどに利用されるICカード10がカードスロット21に挿入可能になっている。

【0022】ICカード10には、課金情報としてクレジットデータ(度数)が格納されサービスを受けるたびに課金の為のクレジットデータを減少する処理が行われる不揮発性メモリ領域11と、ICカードのシリアル番号などのカードにユニークなID:S-IDが記録されたリードオンリーメモリ(ROM)12とが少なくとも備えられている。

【0023】モデム20には、カードスロット21と、モデム機能を有するモデムチップ22と不揮発性メモリ25とがバス26を介して接続される。また、モデムチップ22は、接続端子23を介して電話線などの通信回線24に接続される。

【0024】ゲーム機の本体30には、外部の入力操作装置39との接続を行うI/O部36、外部のテレビモニタ40に画像データを供給するビデオプロセッサ35、外部のゲームプログラムを格納したCDROMやゲームカートリッジなどの記録媒体38からプログラムやデータを読み出す装置37、バックアップ用メモリ3

4、そして、ゲームプログラムや通信プログラムを実行するCPU32、そしてRAM33が、バス41を介して接続される。

【0025】ゲーム機の本体30のモデムスロット31にモデム装置20を装着することで、通信機能付きのゲーム装置となる。そして、必要に応じて、ICカード10がモデム装置20のカードスロット21に装着される。

【0026】図3は、ゲーム機のモデム20内の不揮発性メモリ25内に情報が保存され、それが使用される場合のフローチャートを示す図である。認証用のユーザID:Y-IDとユーザパスワードY-PW及びカードID:S-IDとがモデム20内のメモリ25に保存される場合や、それらの情報がモデム20内のメモリ25から消去される場合には、少なくともICカード10がカードスロット21に装着されることが必要条件である。そうすることにより、店頭などでゲーム機6をサーバ1に接続してのデモを不特定多数の顧客に提供する場合でも、顧客によってそれらの情報が不正に消去されたり書き換えられたりすることを防止する。

【0027】図3に従ってフローチャートを説明する。このフローチャートに示される処理フローは、外部の記録媒体38内に格納されている通信ソフトウェアに従って、ゲーム機の本体10とモデム装置20とにより実現される。

【0028】まず、ステップS10、S12にて、ICカードがモデム装置20のカードスロット21に挿入されているか否か、挿入されている場合に、ICカード内のROMのカードID:S-IDとモデム装置20内の不揮発性メモリ25に記録されているカードID:S-IDとが一致するか否かが判定される。例えば、既にICカード内のカードID:S-IDがモデム20の不揮発性メモリ25内に記録されている場合は、両カードID:S-IDが一致するので、ステップS26にてモデム20内の不揮発性メモリ25に記録されているユーザID:Y-IDとユーザパスワードY-PWとが自動的に送信される。従って、毎回ソフトウェアキーボードからそれらの認証情報である英数字列を入力する必要はない。

【0029】例えば、ICカードが挿入されているが、カードID:S-IDが一致しない場合や、ICカードそのものが挿入されていない場合は、モニタ画面40にユーザIDとユーザパスワードとを入力する画面が表示される(ステップS14)。そこで、ユーザがソフトウェアキーボードから認証に必要な情報であるユーザID:Y-IDとユーザパスワードY-PWとをキー入力する(ステップS16)。そこで、ICカードの挿入を要求するメッセージが表示されてから(S18)、ICカードが挿入されていて(S20)、モデムの不揮発性メモリ25内に情報(認証情報と鍵データ)が記録され

ていないまたはその記録されている情報(認証情報と鍵データ)が入力された情報と一致しない場合(S22)は、ユーザID:Y-ID、ユーザパスワードY-PW、そしてカードID:S-IDの保存、または消去が可能になる(S24)。

【0030】上記のフローチャートに従って、以下異なる操作手順について説明する。

【0031】手順1は、正規ユーザが、初めてICカードをモデム装置に挿入して、認証情報であるユーザID:Y-IDとユーザパスワードY-PW及びICカードのキー情報であるカードID:S-IDを不揮発性メモリ25に記録する場合である。

【0032】この場合は、ステップS10、S12により、カードIDが一致しないと判定され、ステップS14で入力画面が表示され、正規ユーザによりユーザID:Y-IDとユーザパスワードY-PWとが入力される(S16)。この場合は、モデムの不揮発性メモリ25内に認証情報のカードIDやユーザIDやパスワード及び鍵データ等の情報が未書き込みのため(S22)、入力されたユーザID:Y-ID、ユーザパスワードY-PW及び、ICカード内に記録されているカードID:S-ID(鍵データ)が、暗号化されて、モデム20内の不揮発性メモリ25に保存され(S24)、ユーザID:Y-IDとユーザパスワードY-PWとが送信される(S26)。上記の暗号化のキーデータは、通信ソフトウェア内に存在する。

【0033】手順2は、正規ユーザが、上記手順1で登録した後にICカードを挿入して、認証情報の送信を自動で行う場合である。まず、正規ユーザは、正規のICカードを挿入する。ICカード内にROMに記録されているカードID:S-IDが、モデム20の不揮発性メモリ25内に記録されているカードID:S-IDと一致するので(S12)、ステップS26にて、モデムのメモリ25に記録されているユーザID:Y-IDとユーザパスワードY-PWとが送信される。従って、正規ユーザは、毎回認証情報をキー入力する手間を省くことができる。また、正規ユーザは、友人などに認証情報を開示することなくICカードを貸与してサービスを受けることを可能にすることができる。

【0034】手順3は、正規ユーザがICカードを挿入せずに使用する場合である。この場合は、ICカードが挿入されていないので、ステップS14で認証情報の入力画面となり(S14)、正規ユーザは記憶しているユーザID:Y-IDとユーザパスワードY-PWとを入力する(S16)。そして、ICカードが挿入されていないので(S20)、ステップS26にて、入力した認証情報が送信される。この場合は、正規ユーザがICカードを利用しない場合の例である。ICカードを挿入しない限り、モデム内のメモリ25の情報の消去、書換は行われない。

【0035】手順4は、モデムの不揮発性メモリ25内に保存データが存在するが、ICカード内のカードID:S-IDと一致しない場合である。例えば、正規ユーザが新しいICカードを入手した場合である。この場合は、ICカードが挿入されているが(S10)、鍵データであるそのカードID:S-IDとモデム内の不揮発性メモリ25内のカードID:S-IDとが不一致のため(S12)、認証情報の入力画面になり(S14)、ユーザが入力する(S16)。そこで、ICカードが挿入されているが(S20)、モデムの不揮発性メモリ25内の情報が不一致であるので、ユーザがステップ24にてその情報を消去または保存を選択して(S24)、入力した認証情報を送信する(S26)。

【0036】手順5は、正規ユーザが認証情報を変更する場合である。従って、既にモデムのメモリ25には、古い認証情報と鍵データのICカードのカードID:S-IDとが記憶されている。この場合は、最初にICカードを挿入しない。その結果、認証情報入力画面となる(S14)。そこで、正規ユーザが新たな認証情報を入力すると(S16)、ICカードの挿入が促される(S18)。そこで、ICカードを挿入すると、入力した認証情報と書き込み済の認証情報とが不一致であるので、ステップS24にてそれらの情報の消去または入力情報の保存を行うことができる。その後、認証情報が送信される(S26)。この場合も、ICカードを所有する正規ユーザによってのみ情報の消去や保存が可能になる。

【0037】手順6は、第三者が不正に取得したICカードを利用してサーバからサービスを受けようとする場合である。この場合は、ICカードのカードID:S-IDとモデム内のメモリの鍵データであるカードID:S-IDとが不一致となり、自動的に認証情報が送信されることはない。従って、第三者は、正しい認証情報を所有していないので、サーバから認証を受けることはない。

【0038】手順7は、店頭で不特定多数の顧客にデモを提供する場合である。この場合は、例えばモデムに挿入されるICカードを顧客から隔離しておくことで、顧客は認証情報を知ることなく、デモの提供を受けることができる。

【0039】図3のフローチャートに示される通り、最初にICカードの挿入の有無と鍵データの一致とがチェックされる。ICカードが挿入され鍵データであるカードID:S-IDが一致する場合は、認証情報の自動送信を行うが、それ以外の場合は、認証情報の入力画面に移行する(S14)。また、認証情報が入力された後は、ICカードが挿入されていれば(S20)、モデムの不揮発性メモリ25内に書き込まれた情報と入力した情報及び鍵データとが一致しなければ、それらの情報の消去または保存がユーザにより選択される。

【0040】図4は、第一の実施の形態例の変形例を示

す図である。この図は、図1と同じ部分には同じ引用番号を付した。この変形例では、モデム20の不揮発性メモリ25に認証情報であるユーザID:Y-IDとユーザパスワードY-PWとを記録する時、挿入されているICカードのカードID:S-IDを鍵データにして暗号化されたデータが記録される。従って、正規ユーザまたは正規ユーザから正規に貸与された第三者が正規のICカードを挿入した場合にのみ、ICカード内のカードID:S-IDを鍵データにしてモデムの不揮発性メモリに記録された認証情報を復号化して、サーバに送信し、認証を得ることができる。この場合も、サーバに接続する毎に認証情報をキー入力する必要がなく、しかも認証情報はセキュリティの高い方法で記録される。また、第三者に認証情報を開示することなく、ICカードを貸与してサービスの提供を許可することが可能になる。

【0041】[第二の実施の形態例]第二の実施の形態例は、第一の実施の形態例と同様にICカード(通称スマートカード)にユニークに与えられたカードID:S-IDを鍵データとして利用して、経済的価値を有する使用許諾パスワードをゲーム機のメモリに記録することを特徴とする。

【0042】ゲームプログラムに限らず、一般のプログラムの場合でも、プログラムのサンプルまたは一部の使用を許可したプログラムを格納した記録媒体を無償若しくは廉価で流通させ、ユーザがそれを使用して更に全部の機能を利用したい場合に、クレジットカードやプリペイドカードなどの形態で料金を支払い、それを条件に使用できるパスワードを提供することが行われる。この方法であれば、ユーザは自らプログラムまたはゲームを試してみ、気に入ったプログラムまたはその一部分にのみ使用料金を支払うことができ、ユーザの利便性を上げよりプログラムの普及を図ることができる。このような形式において、プログラムやゲームの継続使用できるパスワードは、経済的価値を有し、秘密の状態で使用すべきである。

【0043】ところが、正規のパスワード所有者は、無意味な英数字の文字列からなるパスワードを毎回入力することは煩雑である。更に、この使用許諾パスワードは、複製されることにより第三者がプログラムを使用することができ、無限の経済的価値を生む可能性がある。そこで、第一の実施の形態例と同様に毎回の入力の煩雑さを避ける為に、ゲーム装置や端末装置内の不揮発性メモリにパスワードをICカードのカードID:S-IDを鍵データにして記録して、ICカードを所有する正規のユーザが正規のゲーム機や端末装置にICカードを挿入した場合にのみパスワードの出力が許可される様にする。更に、この使用許諾パスワードを、正規ユーザが所有するICカードのカードID:S-IDを鍵データとして暗号化した形態で、ユーザに提供する。こうするこ

とで、パスワード自体のデータをユーザに知らせずにパスワードの持つ価値をユーザに提供することができる。更に、ICカードの所有をこの使用許諾パスワードの利用の条件とすることで、パスワードのコピーによる不正使用を防止することができ、不正な第三者に対するセキュリティを高くすることができる。

【0044】図5は、第二の実施の形態例の概略図である。この例では、ビデオゲームのプログラムの使用許諾パスワードをゲームパスワードG-PWとしてユーザに与える例である。更に、ビデオゲームで、ロールプレイングゲーム等、ゲーム内に複数のステージが存在し、ユーザが最初のステージから開始して、各ステージをクリアするたびに、次のステージの使用を許諾するゲームパスワードG-PWが必要になる例である。

【0045】まず、サーバ1は、その外部記憶ファイル4に、ゲームID: G-IDとステージID: Stage-IDの組み合わせに対するゲームパスワードG-PWの対応テーブルを記録する。そして、ユーザは、ゲーム機6を通信回線であるネットワークを介してサーバ1に接続し、取得したいゲームパスワードのゲームID: G-IDとステージID: Stage-IDとを、ICカードのカードID: S-IDと共にサーバに送信する。

【0046】サーバ側では、対応テーブルからゲームパスワードG-PWを検出し、そのゲームパスワードG-PWをカードID: S-IDを鍵データとして暗号化し、その暗号化されたゲームパスワードG-PWを、ネットワークを介してゲーム機6に送信する。それと同時にサーバ側は課金処理を行う。ゲーム機6では、モデム20内の不揮発性メモリ内に暗号化されたゲームパスワードG-PWと、その暗号化の鍵データであるカードID: S-IDとを記録する。カードID: S-IDの記録は、第一の実施の形態例の如く、通信プログラムに内蔵された暗号化アルゴリズムで暗号化される。

【0047】その後、ゲーム機6では、ICカードを所有する正規のユーザがICカードをモデム20に挿入した場合に、ICカード10のカードID: S-IDとモデム20のメモリに記録されたカードID: S-IDとを照合し、一致することを条件として、暗号化されたゲームパスワードG-PWをカードID: S-IDを鍵データとして復号化し、そのゲームパスワードG-PWを使用してゲームプログラムの該当する部分を使用可能にする。

【0048】上記の第二の実施の形態例では、第一の実施の形態例と同様に、図2に示されたゲーム本体30、モデム20及びICカード10とが使用される。そして、第一の実施の形態例と同様にして、ICカードのカードID: S-IDが、ゲームパスワードG-PWを読み出す為の鍵データとして使用される。しかも、カードID: S-IDを鍵データに利用してゲームパスワード

を暗号化しているので、ゲームパスワードのコピーによる不正使用に対する耐性は非常に高い。第一の実施の形態例と同様に、正規ユーザが所有するICカードとゲーム機のモデム20とが同時に使用されるときのみ、ゲームパスワードの使用が可能になるので、ゲームパスワードの入力作業を省略することができ、しかも、不正使用に対する耐性が高い。

【0049】第二の実施の形態例の第一の変形例として、ユーザがサーバ1に送るデータとして、ゲームID: G-IDとステージID: Stage-IDとICカードのカードID: S-IDに、さらにICカードのメモリ11に記録されたプリベードデータであるクレジットデータを追加する。サービスの利用料金を予め支払うことで、使用度数を記録したクレジットデータを記録したICカードが提供される。そして、サービスを利用するたびに課金処理として、そのクレジットデータの度数をクレジットダウン（使用度数の減少処理）させることが行われる。即ち、この変形例は、ICカードがプリベードカードとして使用される場合に適用できる。

【0050】この変形例では、更にサーバ側で、カードID: S-IDと最新のクレジットデータとの対応テーブルを外部ファイル7に記録しておく。そこで、サーバ側では、ユーザから送信されるカードID: S-IDとクレジットデータとを、その外部ファイル7内の対応テーブルを参照することにより、正規ユーザからのアクセスであるか否かをチェックする。

【0051】このクレジットデータを送信データに追加することで、ネット上を送信されたゲームID: G-ID、ステージID: Stage-ID、ICカードのカードID: S-ID及びクレジットデータとを不正使用者に盗み見られたとしても、課金によりそのICカードの最近のクレジットデータは減少しているため、クレジットデータをチェックすることで不正使用者からのアクセスであることを検出することができる。また、サーバ側で、ゲームパスワードG-PWを暗号化する鍵データとして、ICカードのカードID: S-ID及びクレジットデータの組を使用することができる。その場合は、クレジットデータが変化するまでの間だけ有効なゲームパスワードG-PWを利用することができる。

【0052】第二の実施の形態例の第二の変形例として、サーバ1は、その外部記憶ファイル5に、カードID: S-IDとその所有者に与えたゲームパスワードG-PWとの対応テーブルを記録する。サーバ1は、課金処理の時に、外部記憶ファイル5にカードID: S-IDと新たに与えるゲームパスワードG-PWとを記録する。従って、一つのカードID: S-IDに対して複数のゲームパスワードが記録されることもある。センタにあるサーバ1の外部ファイル5に、カードID: S-IDと提供したゲームパスワードG-PWとの対応テーブルを記録しておくことで、正規ユーザが正規のICカー

ドを所有していれば、他の場所、他のゲーム機からでもサーバにアクセスしてゲームパスワードG-PWとをダウンロードすることが可能になり、ユーザの利便性を高めることができる。

【0053】図6は、第二の実施の形態例のフローチャート図である。このフローチャート図は、ゲーム機6とサーバ1との間のデータの送受信、それに対するそれぞれの処理内容を示す。

【0054】最初に、ユーザは、サンプルゲームのソフトウェアを入手し、そのサンプルゲームをゲーム機6で実行する(S30)。そして、フリーサンプル部分が終了すると、それから先を使用する為の使用許諾パスワードである、ゲームパスワードが必要になる。そこで、ゲーム機6をセンタのサーバ1に接続し(S32)、個人認証情報と共に、ゲームID:G-ID、ステージID:Stage-ID、ICカードのカードID:S-IDをサーバ1に送信する(S34)。

【0055】それに対して、サーバ1では、個人認証情報のユーザID:Y-IDとユーザパスワードY-PWとをチェックし、認証を行う。そして、正規ユーザであることが確認され、課金処理と共に、ゲームID:G-IDとステージID:Stage-IDに対応するゲームパスワードG-PWをカードID:S-IDを鍵データにして暗号化する(S36)。そして、暗号化されたゲームパスワードG-PWが送られる(S38)。

【0056】ゲーム機6では、モデム20の不揮発性メモリ25内に、その暗号化されたゲームパスワードG-PWと共に、カードID:S-IDを暗号化して記録する(S40)。むろん、ゲームパスワードG-PWに対して、そのゲームID:G-IDとステージID:Stage-IDも記録される。そして、ゲーム機6はサーバ1との通信を切断する(S42)。その後、ゲーム機6では、サーバ1との接続を行うことなく、正規のICカードが挿入されて、その鍵データであるカードID:S-IDが一致する場合のみ、記録されているゲームパスワードG-PWを鍵データで復号化して、必要とするプログラムの使用を可能にする(S44)。

【0057】更に、ICカードのみを所有したユーザが、別の場所の別のゲーム機6からサーバ1に接続して(S46)、認証情報とゲームID:G-ID、そのステージID:Stage-ID及びカードID:S-IDをサーバ1に送信し(S48)、それに対して、サーバ1は、外部記録ファイル5の参照テーブルから、一旦与えられたゲームパスワードをカードID:S-IDを鍵データにして暗号化して、ゲーム機6に送信する(S50)。この場合は、ICカードを所有する正規のユーザは、必要に応じてサーバ1からゲームパスワードをダウンロードすることができる。

【0058】図7は、更に第二の実施の形態例の変形例を示す図である。図7には、図5と同じ引用番号が付さ

れている。上記の第二の実施の形態例では、ゲーム機6のモデム20内の不揮発性メモリ25に、カードID:S-IDを鍵データにして暗号化されたゲームパスワードと共に、その鍵データも記録していた。それに対して、この変形例では、モデム内の不揮発性メモリ25には、鍵データのカードID:S-IDを記録せずに、その鍵データにより暗号化されたゲームパスワードG-PWのみをゲームIDとステージIDに関連付けて記録するだけである。

【0059】そして、ゲームパスワードを利用する時は、挿入されたICカードのカードID:S-IDを鍵データにして記録されたゲームパスワードG-PWを復号化して使用する。正しいICカードが挿入されなければ、正しい復号化されたパスワードが生成されないの、同様に不正利用に対する耐性を高くすることができる。しかも、モデム20内の不揮発性メモリ25内に鍵データを記録しないので、その鍵データが不正に複製されるリスクをなくすることができる。

【0060】この変形例は、図4で示した個人認証情報をカードID:S-IDを鍵データにして暗号化する例と共に利用される時、最も効果大きい。

【0061】

【発明の効果】以上説明した通り、本発明によれば、個人認証情報であるユーザIDとユーザパスワードとを、正規ユーザに配布されるICカードのカードIDを鍵データとしてゲーム機内のメモリに記録する様にしたので、サーバにアクセスするたびに無意味な英数字列の入力を行う必要がなく、しかも、認証情報が記録されるゲーム機のモデムと鍵データが記録されたICカードとを物理的に分離したことで、認証情報が不正に使用されることに対する耐性を高くすることができる。

【0062】更に、本発明によれば、使用許諾パスワードをICカードのカードIDを鍵データに利用して暗号化したデータを、使用許諾パスワードとしてユーザに提供する様にしたので、ユーザに対して使用許諾パスワードそのものを知らせずにサービスを提供することができ、使用許諾パスワードの不正コピーによる不正使用を防止することができる。また、正規ユーザが所有するICカードが挿入された時に、そのカードIDを鍵データにして使用許諾パスワードを復号化することができるようにしたので、不正使用に対する耐性を高くすることができる。

【0063】また、サーバ側で、ICカードの最新のクレジットデータを保管しておくことで、多数の不正使用者がカードID等を送信して使用許諾パスワードの提供を求めても、最新クレジットデータを照合することで、その要求を拒絶することが可能になる。

【図面の簡単な説明】

【図1】第一の実施の形態例の全体構成を示す図である。

【図2】ゲーム機とIDカードの詳細構成を示す図である。

【図3】ゲーム機のモデム内の不揮発性メモリ内に情報が保存され、それが使用される場合のフローチャートを示す図である。

【図4】第一の実施の形態例の変形例を示す図である。

【図5】第二の実施の形態例の概略図である。

【図6】第二の実施の形態例のフローチャート図である。

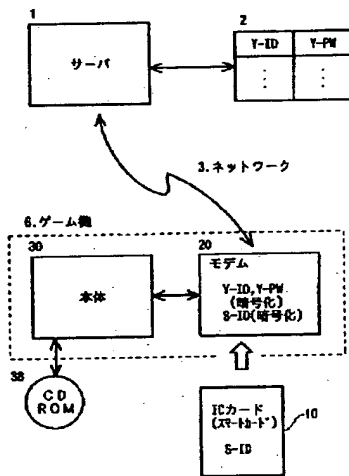
【図7】第二の実施の形態例の変形例を示す図である。*10

*【符号の説明】

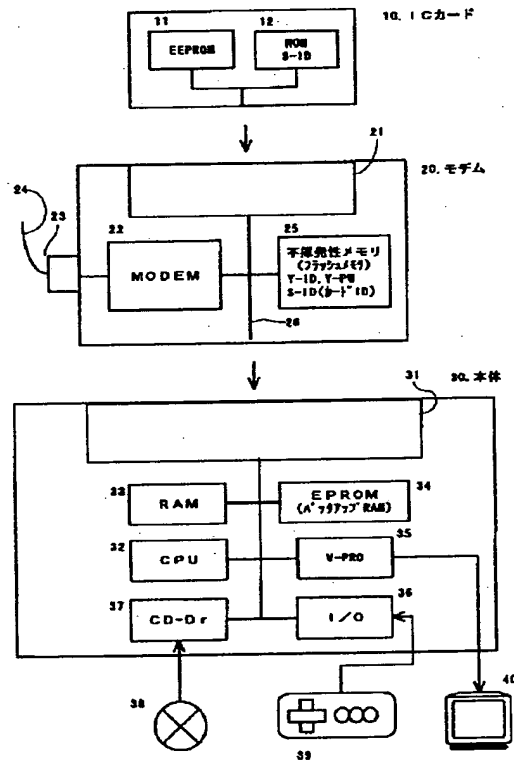
1	サーバ
6	ゲーム機、通信端末装置
10	ICカード
20	モデム
25	不揮発性メモリ、記録媒体
S-ID	カードID
Y-ID	ユーザID
Y-PW	ユーザパスワード
G-PW	ゲームパスワード、使用許諾パスワード

【図1】

第一の実施の形態例の概略図

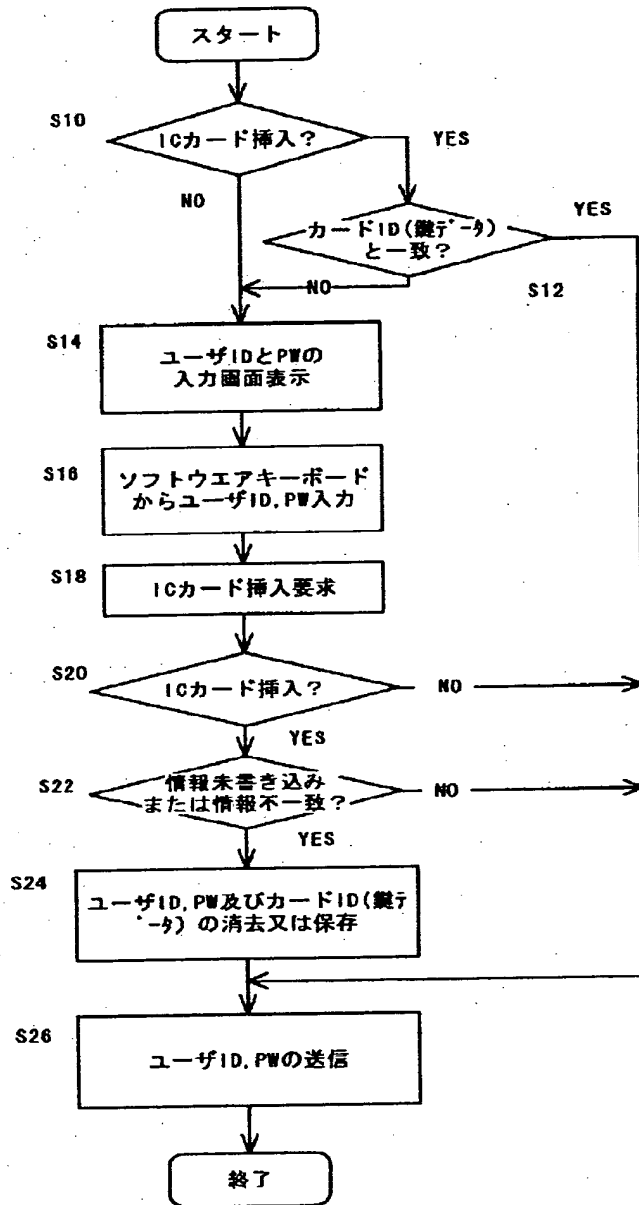


【図2】



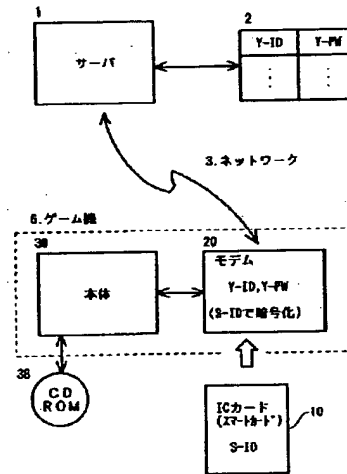
【図3】

第一の実施の形態例のフローチャート図



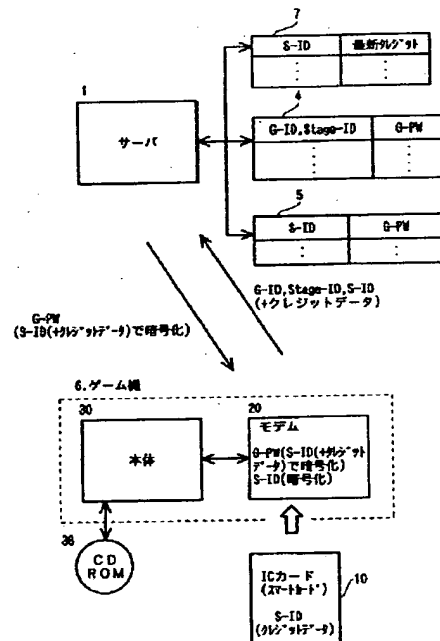
【図4】

第一の実施の形態例の概略図



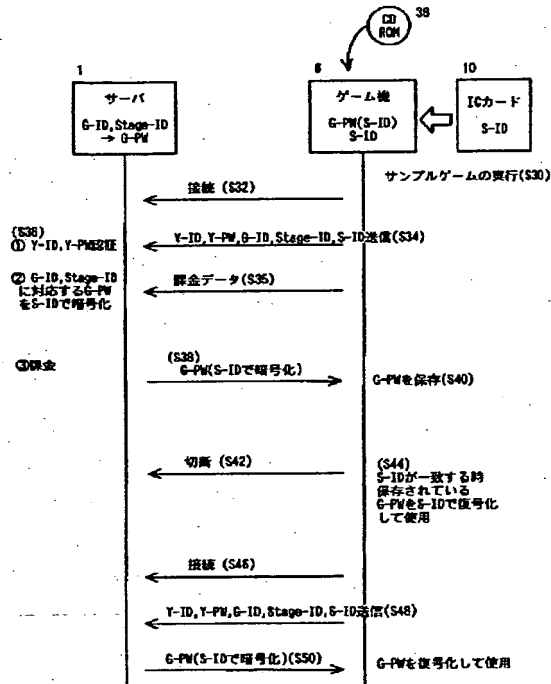
【図5】

第二の実施の形態例の概略図



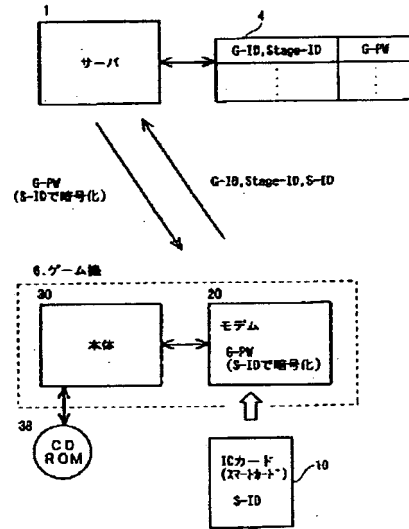
【図6】

第二の実施の形態例のフローチャート図



【図7】

第二の実施の形態例の変形例



フロントページの続き

(51)Int.Cl.⁶

G 0 7 F 7/08

識別記号

F I

G 0 7 F 7/08

S